

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003188873 A

(43) Date of publication of application: 04.07.03

(51) Int. Cl. H04L 9/32  
G09C 1/00

(21) Application number: 2001380971

(22) Date of filing: 14.12.01

(71) Applicant: KANAZAWA INST OF TECHNOLOGY

(72) Inventor: HATTORI MICHIMITSU  
SENGOKU YASUSHI

(54) AUTHENTICATION METHOD, AUTHENTICATION  
DEVICE WHICH CAN UTILIZE THE METHOD,  
USER SYSTEM AND AUTHENTICATION SYSTEM

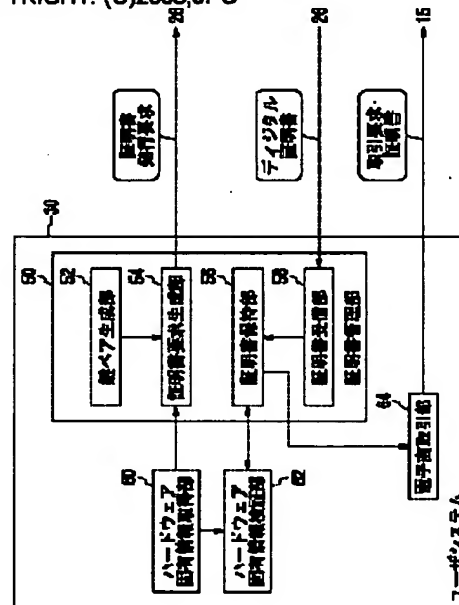
certificate.

COPYRIGHT: (C)2003,JPO

## (57) Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal behavior of a user such as complete faking in e-commerce.

SOLUTION: A hardware characteristics information obtaining part 60 obtains identification information characteristic to hardware utilized by the user. A certificate request generation part 54 transmits the public key of the user generated by a key pair generation part 52 and the characteristic information of the hardware to an authentication device 26 as user information, and a certificate reception part 58 receives a digital certificate having the hardware characteristics information incorporated therein from the authentication device 26 and holds it in a certificate holding part 56. A hardware characteristics information inspection part 62 extracts the hardware characteristics information incorporated in the certificate and detects whether it is coincident with the hardware characteristics information. An e-commerce part 64 performs commerce by using an inspected digital



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-188873

(P2003-188873A)

(43) 公開日 平成15年7月4日 (2003.7.4)

|                           |       |              |                   |
|---------------------------|-------|--------------|-------------------|
| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I          | テーマコード(参考)        |
| H 0 4 L 9/32              |       | G 0 9 C 1/00 | 6 4 0 E 5 J 1 0 4 |
| G 0 9 C 1/00              | 6 4 0 | H 0 4 L 9/00 | 6 7 5 B           |
|                           |       |              | 6 7 3 B           |

審査請求 未請求 請求項の数16 O L (全 12 頁)

(21) 出願番号 特願2001-380971(P2001-380971)

(22) 出願日 平成13年12月14日 (2001.12.14)

特許法第30条第1項適用申請有り 2001年10月31日~11月2日 社団法人情報処理学会 コンピュータセキュリティ研究会主催の「コンピュータセキュリティシンポジウム2001」において文書をもって発表

(71) 出願人 593165487

学校法人金沢工業大学

石川県石川郡野々市町扇が丘7番1号

(72) 発明者 服部 進実

石川県石川郡野々市町扇が丘7番1号 学校法人金沢工業大学内

(72) 発明者 千石 靖

石川県石川郡野々市町扇が丘7番1号 学校法人金沢工業大学内

(74) 代理人 100105924

弁理士 森下 賢樹

Fターム(参考) 5J104 AA07 KA02 KA05 KA10 MA01

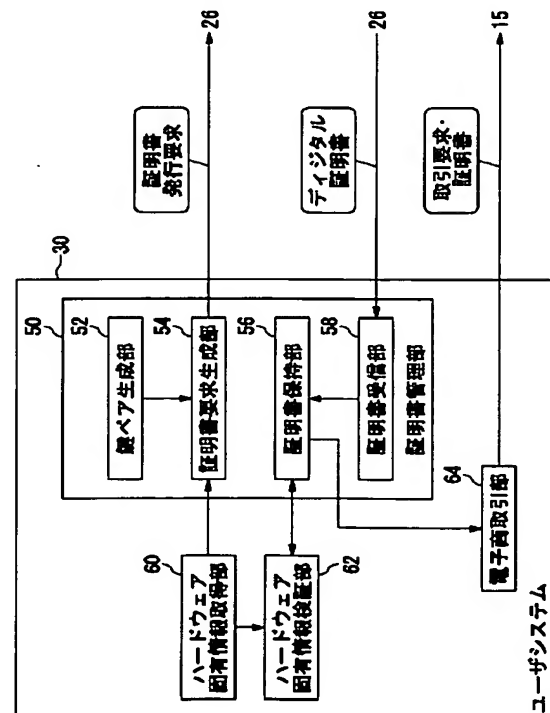
PA10

(54) 【発明の名称】 認証方法、およびその方法を利用可能な認証装置、ユーザシステムおよび認証システム

(57) 【要約】

【課題】 電子商取引において、なりすましなどのユーザの不正行為を防止することは難しかった。

【解決手段】 ハードウェア固有情報取得部60は、ユーザの利用するハードウェアに固有の識別情報を取得する。証明書要求生成部54は、鍵ペア生成部52により生成されたユーザの公開鍵と、当該ハードウェアの固有情報とをユーザ情報として認証装置26に送信し、証明書受信部58は認証装置26からハードウェア固有情報が組み込まれたデジタル証明書を受信し、証明書保持部56に保持する。ハードウェア固有情報検証部62は、証明書に組み込まれたハードウェア固有情報を抽出し、当該ハードウェアの固有情報と一致するかどうか検証する。電子商取引部64は、検証済みのデジタル証明書を用いて商取引を行う。



## 【特許請求の範囲】

【請求項1】 ユーザシステムからデジタル証明書の発行要求が出されたとき、そのユーザシステムで利用するハードウェアに固有の識別情報を組み込む形で当該証明書を生成し、そのユーザシステムへ発行することを特徴とする認証方法。

【請求項2】 前記ユーザシステムは、自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証した後、ネットワーク上の電子商取引の際にその証明書を利用することを特徴とする請求項1に記載の認証方法。

【請求項3】 ネットワーク上で前記ユーザシステムに所定のサービスを提供する組織が前記証明書の発行機関を兼ねることを特徴とする請求項1または2に記載の認証方法。

【請求項4】 前記ハードウェアに固有の前記識別情報を標準的なデジタル証明書の拡張領域に埋め込んで発行することを特徴とする請求項1から3のいずれかに記載の認証方法。

【請求項5】 前記ユーザシステムは、前記証明書の発行要求の際、自己のハードウェアに固有の識別情報を読み出し可能に設定することを特徴とする請求項1から4のいずれかに記載の認証方法。

【請求項6】 前記ユーザシステムは、前記証明書の発行要求に先立ち、ユーザに自己のハードウェアに固有の識別情報を読み出してよいかどうか問い合わせることを特徴とする請求項1から5のいずれかに記載の認証方法。

【請求項7】 ユーザシステムで利用するハードウェアに固有の識別情報を組み込む形でデジタル証明書を生成する証明書生成部と、前記生成された証明書を前記ユーザシステムに発行する証明書発行部と、前記証明書を保持する証明書データベースとを含むことを特徴とする認証装置。

【請求項8】 第3者から前記証明書の正当性を検証するための公開鍵を要求されたとき、前記証明書データベースから当該証明書の公開鍵を抽出して配布する公開鍵配布部をさらに含むことを特徴とする請求項7に記載の認証装置。

【請求項9】 ユーザが利用する自己のハードウェアに固有の識別情報を取得する取得部と、前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだデジタル証明書の発行を受け、その証明書を保持する証明書管理部と、前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証する検証部とを含むことを特徴とするユーザシステム。

【請求項10】 前記検証された証明書を利用して電子商取引を要求する取引部をさらに含むことを特徴とする

請求項9に記載のユーザシステム。

【請求項11】 前記検証部により前記証明書の正当性が否定された場合、前記証明書を用了電子商取引を禁止し、前記認証局にその旨を通知する警告部をさらに含むことを特徴とする請求項10に記載のユーザシステム。

【請求項12】 前記取得部は、前記自己のハードウェアに固有の識別情報の読み出し許可をユーザから得た上で、その識別情報を取得することを特徴とする請求項9から11のいずれかに記載のユーザシステム。

【請求項13】 デジタル証明書を発行する認証装置と、前記証明書の発行を受けるユーザシステムとを含む認証システムであって、

前記認証装置は、

前記ユーザシステムで利用するハードウェアに固有の識別情報を受信し、その識別情報を組み込む形でデジタル証明書を生成する証明書生成部と、

前記生成された前記証明書を前記ユーザシステムに発行する証明書発行部と、

前記証明書を保持する証明書データベースとを含み、

前記ユーザシステムは、

ユーザが利用する自己のハードウェアに固有の識別情報を取得する取得部と、

前記自己のハードウェアに固有の識別情報を前記認証装置に送信して、その識別情報を組み込んだデジタル証明書の発行を受け、その証明書を保持する証明書管理部と、

前記自己のハードウェアに固有の識別情報と照合して前記証明書の正当性を検証する検証部とを含むことを特徴とする認証システム。

【請求項14】 ユーザが利用する自己のハードウェアに固有の識別情報を取得するモジュールと、

前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだデジタル証明書の発行を受け、その証明書を保持するモジュールと、

前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証するモジュールとを含むコンピュータ用のプログラム。

【請求項15】 証明書発行の申請時に、ユーザシステムは自己が使用しているハードウェアの固有情報を含めた個人情報を認証局に送り、前記認証局は、その情報を付加した証明書を発行し、前記ユーザシステムは受け取ったデジタル証明書を使用して認証を行い、電子商取引を行うことを特徴とする認証システム。

【請求項16】 前記ユーザシステム側でユーザの使用しているハードウェア情報と証明書に記録されているハードウェア情報を比較し、一致すれば、その証明書を前記電子商取引におけるサービス提供者側に送信し、前記サービス提供者側でその証明書の認証を行い、取引を開始することを特徴とする請求項15に記載の認証システム。

ム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はユーザの不正行為を抑制する認証技術、とくにデジタル証明書を利用してユーザのなりすましなどの不正行為を抑制する認証方法およびその方法を利用可能な認証装置、ユーザシステムおよび認証システムに関する。

【0002】

【従来の技術】近年、インターネット上での電子商取引が盛んに行われるようになってきている。その一つとしてオンラインショップを利用するオンラインショッピングがある。このオンラインショッピングはいわゆる「通信販売」であるが、インターネットを利用している人にとっては通信販売以上に簡単に商品を注文・購入できたり、サービスを受けたりすることができる有意義なものである。

【0003】また電子署名を用いて各種公的手続きをネットワーク上で行うことも時代の趨勢であり、日本でも今年から電子署名法が施行され、電子政府構想が政策として掲げられている。近い将来、公的書類の申請や発行、税金等の手続きが電子的に行われるようになると期待されている。

【0004】

【発明が解決しようとする課題】しかし、いくつかの問題点も抱えている。オンラインショッピングの問題には、電子商取引における不正行為が挙げられる。その不正行為には、オンラインショップ側の不正とユーザ側の不正がある。ショップ側の不正行為として、商品の未着、代金引換郵便の悪用などがある。またユーザ側の不正行為には、不当なID・パスワードの使用、クレジットカードの盗用などの「なりすまし」がある。

【0005】不正に入手したユーザIDとパスワードを用いて海外からローミングサービスを利用したり、インターネットで利用したクレジットカード番号が盗用されるなどなりすましによる不正アクセス事件のニュースが数多く報告されている。そのような事件が多発する中で、オンラインショップ側の不正行為はショップを利用するユーザ側が注意することである程度防ぐことが出来るが、ユーザ側の不正行為を防ぐことは非常に困難であると考えられる。

【0006】本発明はこうした状況に鑑みてなされたものであり、その目的は、ユーザの匿名性を残しつつ、ユーザを間接的に証明する情報を付加したデジタル証明書を利用して認証を行い、ユーザの不正行為を抑制する認証技術を提供することにある。

【0007】

【課題を解決するための手段】本発明のある態様は認証方法に関する。この方法は、ユーザシステムからデジタル証明書の発行要求が出されたとき、そのユーザシ

テムで利用するハードウェアに固有の識別情報を組み込む形で当該証明書を生成し、そのユーザシステムへ発行する。

【0008】前記ユーザシステムは、自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証した後、ネットワーク上の電子商取引の際にその証明書を利用してもよい。

【0009】ネットワーク上で前記ユーザシステムに所定のサービスを提供する組織が前記証明書の発行機関を兼ねてもよい。この組織は、ユーザシステムにインターネットへの接続サービスを提供するインターネットサービスプロバイダであってもよい。またこの組織は専用線を引いている企業や団体であってもよい。このような組織はサービスをユーザに無償または有償で提供し、ユーザの個人情報や管理している。この証明書の発行機関は、前記ハードウェアに固有の前記識別情報を標準的なデジタル証明書の拡張領域に埋め込んで発行してもよい。ハードウェアに固有の識別情報は、ユーザシステムと証明書の発行機関との間で一意性が保証されるものであってもよい。

【0010】前記ユーザシステムは、前記証明書の発行要求の際、自己のハードウェアに固有の識別情報を読み出し可能に設定してもよい。前記ユーザシステムは、前記証明書の発行要求に先立ち、ユーザに自己のハードウェアに固有の識別情報を読み出してよいかどうか問い合わせてもよく、ユーザが読み出しを許可した場合に、識別情報の読み出しが可能になるように設定を行ってもよい。

【0011】本発明の別の態様は認証装置に関する。この装置は、ユーザシステムで利用するハードウェアに固有の識別情報を組み込む形でデジタル証明書を生成する証明書生成部と、前記生成された証明書を前記ユーザシステムに発行する証明書発行部と、前記証明書を保持する証明書データベースとを含む。第3者から前記証明書の正当性を検証するための公開鍵を要求されたとき、前記証明書データベースから当該証明書の公開鍵を抽出して配布する公開鍵配布部をさらに含んでもよい。

【0012】本発明のさらに別の態様はユーザシステムに関する。このユーザシステムは、ユーザが利用する自己のハードウェアに固有の識別情報を取得する取得部と、前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだデジタル証明書の発行を受け、その証明書を保持する証明書管理部と、前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証する検証部とを含む。

【0013】前記検証された証明書を利用して電子商取引を要求する取引部をさらに含んでもよい。前記検証部により前記証明書の正当性が否定された場合、前記証明書を用了電子商取引を禁止し、前記認証局にその旨を

通知する警告部をさらに含んでもよい。

【0014】前記取得部は、前記自己のハードウェアに固有の識別情報の読み出し許可をユーザから得た上で、その識別情報を取得してもよい。

【0015】本発明のさらに別の態様は認証システムに関する。この認証システムは、前述の認証装置とユーザシステムとを含む。

【0016】本発明のさらに別の態様はコンピュータ用のプログラムに関する。このプログラムは、ユーザが利用する自己のハードウェアに固有の識別情報を取得するモジュールと、前記自己のハードウェアに固有の識別情報を認証局に送信して、その識別情報を組み込んだデジタル証明書の発行を受け、その証明書を保持するモジュールと、前記自己のハードウェアに固有の識別情報と照合して前記発行された証明書の正当性を検証するモジュールとを含む。

【0017】本発明のさらに別の態様も認証システムに関する。証明書発行の申請時に、ユーザシステムは自己が使用しているハードウェアの固有情報を含めた個人情報を認証局に送り、前記認証局は、その情報を付加した証明書を発行し、前記ユーザシステムは受け取ったデジタル証明書を使用して認証を行い、電子商取引を行う。前記ユーザシステム側でユーザの使用しているハードウェア情報と証明書に記録されているハードウェア情報を比較し、一致すれば、その証明書を前記電子商取引におけるサービス提供者側に送信し、前記サービス提供者側でその証明書の認証を行い、取引を開始してもよい。

【0018】なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、サーバ、システム、コンピュータプログラム、記録媒体などの間で変換したものもまた、本発明の態様として有効である。

【0019】

【発明の実施の形態】本発明の目的は、電子商取引において、ユーザ側の不正行為である「なりすまし」を事前に防ぐことである。このなりすましは、インターネット上での高い匿名性という性質を悪用した行為であるが、実施の形態ではユーザの匿名性は残しつつユーザの不正行為を抑制する方法を提案する。

【0020】現在、Webでは幾つかの認証システムが利用されている。主なものにインターネットを通じて安全にクレジットカード決済を行うためのSET (Secure Electronic Transactions) や米国マサチューセッツ工科大学でのAthenaプロジェクトの一部として設計された認証システムであるKerberosなどがある。

【0021】これらの認証システムは通信中のデータの安全を確保するためのシステムであり、ユーザ自身が不正なユーザアカウントやパスワードを使用していることを検出するのは困難であり、また不正行為を検出した場

合でもそのユーザを突き止めることは困難である。

【0022】不正行為を抑制するためにはユーザの個人情報情報を公開すればいいが、ある程度個人の匿名性を残すために、直接的にはユーザを知ることができないが間接的にはユーザを知ることのできる情報を公開することとする。公開する情報は第三者によって改竄されたり、盗用されないようにデジタル証明書を使用する。そのユーザを間接的に知ることができる情報をデジタル証明書に付加して利用し、ユーザの認証を行うことによりユーザの不正行為を抑制させる。つまり、善良なサービス提供者である店舗を保護しながら、ユーザが安全な電子商取引を行うためのWeb認証システムを提案する。

【0023】実施の形態に係る認証システムを説明する前に、既存の認証システムを説明する。認証システムは多くの種類が存在しているが、それらのシステムで用いられている既存の認証方法は次のように分類できる。

【0024】(1) 変形パスワード

パスワードを一方方向性関数を通して処理し、ホストが記憶していたパスワードに同じ関数を適用し、2つを比較することにより認証を行う。通信中の盗聴を防ぐ。

【0025】(2) チャレンジ応答

ホストがユーザにチャレンジと呼ぶランダム値を送り、その値を一方方向性関数で計算し、返答とともに戻す。暗号化されたパスワードをそのまま用いる再生攻撃に対抗する。

【0026】(3) タイムスタンプ

認証要求時に現在の日時を用いる。すべてのシステムが安全で同期がとれている時計を持っている必要がある。

【0027】(4) ワンタイムパスワード

変形パスワードの一種で、パスワードに一方方向性関数を用いて一度しか使えないパスワードを生成する。盗聴と再生攻撃の両方に対抗する。

【0028】(5) ゼロ知識法

会話型証明システムに基づく暗号技術のひとつである。

【0029】(6) デジタル署名またはデジタル証明書

認証プロトコルの基本である。データの一部をユーザの私有鍵を用いて署名し、私有鍵の持ち主であることを証明する。

【0030】また、主な認証システムとして、SETとKerberosが挙げられる。SETは、インターネットを通じて安全にクレジットカード決済を行うための技術仕様である。大手クレジットカード会社のほか、コンピュータ関連企業が協同で規格を策定している。SETの使用目的は、クレジットカード番号がショップに知られないようにすることである。

【0031】ユーザがSETを利用するには、専用ソフトウェアをダウンロードしなければならず、そのソフトウェアをユーザが入手するにはWeb上でのSET利用申請が必要で、その申請にはインターネット上で情報を

10

20

30

40

50

暗号化して送受信するプロトコルであるSSL (Secure Socket Layer) が利用されている。また、専用ソフトウェアさえ使用していれば正規のユーザとみなされる。

【0032】したがってSETには、(1) 専用のソフトウェアを使用する必要がある、(2) 正規ユーザ認証が申請時すなわち専用ソフトダウンロード時の一回だけである、(3) 汎用性があまりないなどの問題があり、「なりすまし」の対策が不十分であると考えられる。

【0033】Kerberosとは、マサチューセッツ工科大学のAthenaプロジェクトで開発されたネットワーク上で利用を前提としたユーザ認証方式のことである。Kerberos認証では、認証サーバ(AS: Authentication Server)と鍵配布サーバ(TGS: Ticket Granting Server)の2つのサーバによって認証が行われ、通信の秘匿やユーザ認証などをすべて共通鍵暗号で実現しているのが特徴である。

【0034】SETやKerberosは通信中にID・パスワードや秘密情報が傍受されることを防いでいるが、秘密情報が盗まれてしまえば機能しなくなる。だが、次に述べる実施形態の認証システムでは、ユーザの使用しているハードウェアに関する情報を基に認証を行うため、ハードウェア自身が盗まれない限り、安全に認証を行える。情報が盗まれた時よりも、物自体が盗まれた時の方が発見が早いので、本実施形態の認証システムでは不正行為による被害を最小限に止めることが出来る。

【0035】本認証システムは、デジタル証明書を利用したWeb認証システムである。デジタル証明書にユーザを間接的に知ることの出来る情報を新たに付加することにより、認証を強化する。ユーザを間接的に知る情報として、ユーザが使用しているハードウェアの固有な情報を利用することとする。そのハードウェア固有情報を証明書に付加して、接続時に証明書による認証を行う。

【0036】本認証システムで使用するデジタル証明書は、X. 509バージョン3証明書に準拠している。

【0037】標準公開鍵証明書の形式であるX. 509証明書形式は、次のようなものである。

(1) ISO (国際標準化機構)、IEC (国際電気標準会議)、ITU (国際電気通信連合) が定めた標準公開鍵証明書形式である。

(2) 1988年にバージョン1が開発され、現在はバージョン3が使用されている。

(3) バージョン3において拡張領域が追加されている。

(4) 他の機能として証明書の有効期限等を設定することができ、扱いやすいデジタル証明書である。

【0038】また、X. 509証明書の構造は次のようになっている。なお以下においてX. 500とは、データ通信網、特にメッセージ通信網におけるディレクトリ

機能を標準化することを目指してITU-Tが1988年に勧告したものであり、X. 509証明書では、認証局や証明書の保持者などのエンティティの名前として、このX. 500標準を用いてインターネット全体での一意性を保つ。

【0039】1. 証明書バージョン

X. 509による証明書のバージョン番号

2. 証明書シリアル番号

認証局より任意に割り当てられた番号

3. アルゴリズム識別子

証明書発行者の署名用のデジタル署名アルゴリズムの識別子

4. 認証局のX. 500名前

発行者である認証局のX. 500名前

5. 有効期限

証明書の開始および終了日時

6. 主体者のX. 500名前

証明される公開鍵と関連する私有鍵の保有者のX. 500名前

7. 主体者の公開鍵情報

主体者すなわち証明書使用者の公開鍵値とそれに使われているRSA、楕円暗号等のアルゴリズムの識別子

8. 認証局の識別子

証明書を発行する認証局の名前があいまいにならないようにするために用いるオプションビット列

9. 主体者の識別子

主体者の名前があいまいにならないように用いるオプションビット列

10. 拡張

拡張領域

11. 認証局のデジタル署名

ハッシュアルゴリズムを用いて証明書のダイジェストすなわち指紋に相当するデータを取り、そのダイジェストを認証局の秘密鍵によって暗号化したもの。

【0040】図1は、X. 509証明書に含まれるこれらのデータの構造を説明する図である。本認証システムは、X. 509証明書の拡張領域にハードウェア固有情報を付加した独自の証明書による認証を行う。

【0041】本認証システムにおいて、デジタル証明書に付加するハードウェア情報は以下のものを利用する。

(1) PSN (Processor Serial Number)

(2) MACアドレス (Media Access Control Address)、IPアドレス (Internet Protocol Address)

【0042】MACアドレスやIPアドレスの情報は不正に書き換えられる恐れがあるため、書き換え不可能で固有のハードウェア情報であるPSNを利用することが重要である。

【0043】PSNはIntel社がペンティアム3 (登録商標) 以降のマイクロプロセッサに搭載したプロ

セッサ固有の識別番号である。すべてのチップに違う番号が割り当てられ、コンピュータの識別に使われる。

【0044】このPSNを表示及び使用するには、インテルプロセッサシリアルナンバーコントロールユーティリティ (Intel Processor Serial Number Control Utility) を使用する。BIOSの設定で無効になっていれば、マザーボードの「Processor Number Feature」を「Enabled」にしておかなければ、警告のダイアログが表示され「無効」のままである。

【0045】図2のように、プロセッサシリアルナンバーコントロールユーティリティを起動すると、BIOSの設定が有効になっていれば、96ビットのプロセッサシリアルナンバーが表示される。

【0046】MACアドレスとは、各Ethernet (登録商標) カードに固有のID番号である。全世界のEthernetカードには1枚1枚固有の番号が割り当てられており、これを元にカード間のデータの送受信が行われる。

【0047】IPアドレスは、インターネットやイントラネットなどのIPネットワークに接続されたコンピュータ1台1台に割り振られた識別番号である。

【0048】本認証システムはWeb上での電子商取引で使用するにより、電子商取引での不正行為の一つである「なりすまし」の抑制を目的としている。なりすまし等の不正行為を抑制させるために、デジタル証明書にユーザを間接的に知ることの出来るハードウェア固有情報を付加させている。しかし、これだけでは不正行為を抑止することは困難であり、ハードウェア固有情報を付加したデジタル証明書を使用した認証システムを効果的に運用・利用する必要がある。

【0049】ユーザの不正行為を抑制させるために認証システムを効果的に運用するには、ISP (Internet Services Provider) や専用線を引いている各種団体を認証局 (CA: Certificate Authority) として利用する方法が考えられる。ほとんどのユーザは各自のコンピュータをインターネットに接続するためにISPや専用線を引いている各種団体を利用しているため、ISPや専用線を引いている各種団体をCAとして証明書の発行・管理を行う。

【0050】ISPや各種団体等がCAとなることで、証明書を持っているユーザの身元を管理することが容易である。また、CA機関を新たに設ける必要がないため、コストや普及の面でもメリットがある。

【0051】また、ISPや各種団体等に不正防止の責任義務を持たせることで、ユーザの不正行為をさらに抑制することが出来ると考えられる。

【0052】本認証システムは、主にWeb上の電子商取引での利用を目的としている。つまり、Web上のオンラインショッピングで、ユーザが不正行為を行わないようにするための認証システムである。

【0053】図3は、デジタル証明書の申請と発行の手順を説明する図である。まず、ユーザはユーザ自身が所属しているISP等に証明書発行の申請をする。その申請時に、ユーザは自身が使用しているコンピュータのMACアドレス、PSNを含めた個人情報をCAであるISPに送る。CAは、その情報を基に証明書を発行する。そして、ユーザは受け取ったデジタル証明書を使用して認証を行い、電子商取引を行う。

【0054】図4は、認証システムにおける商取引の手順を説明する図である。サービスを提供する側であるオンラインショッピング店舗等は、利用者が接続して送信してくるデジタル証明書を基に利用者の認証を行い、取引を行う。

【0055】CAより発行されたデジタル証明書は、ユーザ側のコンピュータ内で保存管理される。例え不正をしようとしても、デジタル証明書は改竄されたり不正生成されることはない。

【0056】図5は、証明書の管理と認証の手順を説明する図である。ユーザがオンラインショッピングなどを利用する時、まずユーザ側でユーザの使用しているハードウェア情報と証明書に記録されているハードウェア情報を比較する。一致すれば、その証明書をサービス提供者側に送信する。受け取った提供者側でその証明書の認証を行い、取引を開始する。

【0057】これらの動作は、ユーザ、サービス提供者共に本認証システムの専用ソフトウェアで行う事とする。この専用ソフトウェアはCAによって完全性を認証する。

【0058】本認証システムの仕様をまとめると以下の通りである。

- (1) デジタル証明書を利用した認証システム。
- (2) デジタル証明書形式はISO/IEC/ITUが定めたX.509標準バージョン3を使用。
- (3) デジタル証明書の拡張としてコンピュータ固有の情報を付加させる。
- (4) 固有の情報としてPSN、MACアドレス、IPアドレスを使用する。
- (5) プラットフォームはパーソナルコンピュータの標準的なOSである。
- (6) ソフトウェアは標準的なC++言語の開発環境で開発される。
- (7) ISPや専用線を引いている各種団体をCAとすることで、不正行為抑制を強化。

【0059】図6は、実施の形態に係る認証システムの構成図である。オンラインショッピングサイト10は、オンラインにより商品の販売を行うサイトであり、Webサーバ12、データベースサーバ14、およびショッピングシステム15を含む。ユーザはWebサーバ12にアクセスして商品の閲覧、購入の申し込みができる。データベースサーバ14はWebサーバ12と連携して商品



の購入履歴の管理やユーザの個人情報の管理などを行う。ショッピングシステム15は、証明書を利用したユーザ認証を行う専用ソフトウェアである。このショッピングシステム15は、Webサーバ12またはデータベースサーバ14の機能の一部として設けられてもよい。なおオンラインショッピングサイト10にはファイアウォールなどの機能が当然に含まれるが、ここでは図示しない。

【0060】インターネットサービスプロバイダ18は、ユーザ端末28にインターネット16へのアクセス環境を提供するものであり、メールサーバ20、DNSサーバ22、プロキシサーバ24、および認証装置26を含む。ユーザ端末28は図示しないアクセスポイントにダイヤルアップなどで接続し、インターネットサービスプロバイダ18が提供する電子メール、インターネットアクセスなどのサービスを利用する。またユーザ端末28に搭載された専用ソフトウェアであるユーザシステム30は、インターネットサービスプロバイダ18内の認証装置26と通信して証明書の発行を受ける。このようにインターネットサービスプロバイダ18はユーザ端末28を認証する認証局としての機能を兼ね備える。

【0061】図7は、認証装置26の構成図である。この構成は、ハードウェア的には、任意のコンピュータのCPU、メモリ、その他のLSIで実現でき、ソフトウェア的にはメモリにロードされた認証機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。

【0062】証明書生成部32は、ユーザシステム30から証明書発行要求を受け取り、デジタル証明書を生成する。ユーザシステム30から受け取る証明書発行要求には、ユーザの利用するハードウェアすなわちユーザ端末28に固有の識別情報が含まれる。

【0063】証明書生成部32は、鍵生成部34、ダイジェスト生成部36、およびデジタル署名部38を含む。ダイジェスト生成部36は証明書データをハッシュ関数に通してダイジェストを取得する。証明書データは、証明者情報、認証局情報、ユーザ情報、および拡張情報を含む。証明者情報は、図1で説明した(1)証明書バージョン、(2)証明書シリアル番号、(3)アルゴリズム識別子、および(5)有効期限のデータであり、認証局情報は、(4)認証局のX.500名前および(8)認証局の識別子のデータである。ユーザ情報は、(6)主体者のX.500名前、(7)主体者の公開鍵情報、および(9)主体者の識別子のデータである。また拡張情報は、(10)拡張領域のデータである。また拡張情報にはユーザシステム30から受け取ったハードウェア固有情報が含まれる。したがって、証明

書データにはユーザが利用しているハードウェアの固有情報が組み込まれている。

【0064】デジタル署名部38は、鍵生成部34が生成した当該認証局の秘密鍵を用いて、ダイジェスト生成部36により生成されたダイジェストを暗号化してデジタル署名を生成し、その署名データを図1のように証明書データに追加する。なお鍵生成部34が生成した当該認証局の公開鍵と秘密鍵のペアは証明書データベース42に保持される。証明書発行部40は、このようにして生成されたデジタル証明書を証明書データベース42に保持するとともに、ユーザシステム30へ発行する。

【0065】公開鍵配布部44は、ショッピングシステム15から当該認証局の公開鍵の要求を受け付け、証明書データベース42から当該認証局の公開鍵を取得してショッピングシステム15へ送信する。

【0066】図8は、ユーザシステム30の構成図である。この構成図は、ソフトウェアとハードウェアの連携によって実現される機能ブロックを描いたものであり、これらの機能ブロックは、ユーザ端末28にインストールされるアプリケーションプログラムとして実現されてもよく、少なくとも一部がオペレーションシステムやファームウェアの機能を用いて実現されたり、ハードウェアを用いて実現されてもよい。

【0067】証明書管理部50は、認証装置26へ証明書発行要求を送信し、認証装置26からデジタル証明書を受信して管理する。証明書管理部50は、鍵ペア生成部52、証明書要求生成部54、証明書保持部56、および証明書受信部58を含む。鍵ペア生成部52は、ユーザ固有の公開鍵と秘密鍵のペアを生成する。生成された鍵は図示しない記憶部に保持される。ハードウェア固有情報取得部60は、当該ユーザシステム30がインストールされたハードウェアすなわちユーザ端末28に固有の識別情報を取得する。このハードウェア固有の識別情報の一例は、前述のPSNであり、MACアドレス、IPアドレスなどで代用したり、組合せてもよい。

【0068】証明書要求生成部54は、鍵ペア生成部52により生成された公開鍵と、ハードウェア固有情報取得部60により取得されたハードウェア固有情報とをユーザ情報として用いた証明書発行要求を生成し、認証装置26にその要求を送信する。

【0069】証明書受信部58は認証装置26が発行したデジタル証明書を受信し、証明書保持部56がそのデジタル証明書を保持する。ハードウェア固有情報検証部62は、証明書保持部56に保持されたデジタル証明書に組み込まれたハードウェア固有情報を抽出し、ハードウェア固有情報取得部60により取得された自己のハードウェア固有情報と比較し、両者が一致するかどうかを検証する。電子商取引部64は、ショッピングシステム15との間で電子商取引を開始する際、証明書保持部



56に保持された検証済みのデジタル証明書をショッピングシステム15に送信する。ショッピングシステム15は後述のようにユーザシステム30から送信されたデジタル証明書を検証して、電子商取引部64に取引の開始確認を返信する。これを受けて電子商取引部64はショッピングシステム15との間で商取引を行う。

【0070】ハードウェア固有情報検証部62による検証の結果、デジタル証明書に含まれるハードウェア固有情報と当該ユーザ端末28のハードウェア固有情報とが一致しなかった場合、ハードウェア固有情報検証部62はそのデジタル証明書が不正に入手されたものと判断して無効化し、電子商取引部64による商取引に使用されないように制限する。またそのような場合、認証局に不正があることを通知する警告部がさらに設けられてもよい。

【0071】図9は、ショッピングシステム15の構成図である。電子商取引部70は、ユーザシステム30からデジタル証明書とともに取引要求を受け取る。CA公開鍵管理部74は、デジタル証明書を発行した認証装置26に対してCA固有の公開鍵を要求し、認証装置26からそのCA公開鍵を受け取る。証明書検証部72は、CA公開鍵を用いて、電子商取引部70が受信したデジタル証明書を復号し、証明書の正当性を検証する。証明書が検証されると、電子商取引部70はユーザシステム30へ取引開始確認を送信する。これ以降、電子商取引部70はユーザシステム30との間で商取引を行う。証明書の正当性が確認されなかった場合は、ユーザシステム30の取引要求を拒否する。

【0072】図10～図13を参照して、実施の形態に係る認証システムによる認証手順を説明する。図10は、認証装置26におけるデジタル証明書の生成と発行の手順を示すフローチャートである。証明書生成部32はユーザから証明書発行要求を受信する(S10)。この発行要求にはユーザが利用しているハードウェアに固有の識別情報が含まれている。ダイジェスト生成部36は、このハードウェア固有情報を含むデジタル証明書のデータをハッシュ関数に通してダイジェストを生成する(S12)。ダイジェストはデジタル証明書の「指紋」に相当する。デジタル署名部38は当該認証局の秘密鍵を用いてこのダイジェストを暗号化して署名データを作成し、デジタル証明書に付加する(S14)。証明書発行部40はこうして得られたデジタル証明書を発行する(S16)。

【0073】図11は、ユーザシステム30における証明書発行要求の手順を示すフローチャートである。鍵ペア生成部52はユーザ固有の公開鍵と秘密鍵のペアを生成する(S20)。ハードウェア固有情報取得部60はハードウェア固有情報を読み出してもよいかどうかユーザに問い合わせる(S22)。ユーザが読み出しを許可した場合(S22のY)、ハードウェア固有情報取得部

60はハードウェア固有情報を取得する(S24)。証明書要求生成部54は取得したハードウェア固有情報とユーザの公開鍵データをユーザ情報として含むデジタル証明書の発行要求を認証装置26に送信する(S26)。ステップS22でユーザが読み出しを許可しない場合(S22のN)、ハードウェア固有情報の読み出しおよび証明書の発行要求をすることなく、終了する。

【0074】なお、鍵の生成(S20)は証明書の発行要求のたびに行う必要はなく、一度生成した鍵を何度も用いてよい。またハードウェア固有情報の読み出しの問い合わせ(S22)についても、ユーザが一度読み出しを許可すると、再度の問い合わせをしないようにしてもよい。またハードウェア固有情報の読み出しができないようにロックをかけ、ユーザが読み出しの許可を与えた場合にそのロックを解除して自由に読み出し可能にするロック制御部をさらに設けてもよい。

【0075】図12は、ユーザシステム30におけるハードウェア固有情報の検証手順を示すフローチャートである。認証装置26からデジタル証明書が受信されると、CAの公開鍵を用いてその証明書の正当性が検証される(S30)。ハードウェア固有情報検証部62は証明書からハードウェア固有情報を抽出する(S32)。ハードウェア固有情報取得部60は当該ユーザシステム30が利用するハードウェアから自己のハードウェア固有情報を取得する(S34)。ハードウェア固有情報検証部62は、証明書から抽出されたハードウェア固有情報と自己のハードウェア固有情報とを比較し、一致するかどうかを調べる(S36)。一致する場合(S36のY)、電子商取引部64は商取引の要求の際、そのデジタル証明書をショッピングシステム15に送信し(S38)、一致しない場合(S36のN)、デジタル証明書の送信を行わない。一致しない場合、そのデジタル証明書は不正に入手されたものである可能性があるため、その証明書を発行したCAである認証装置26に不正があることを警告するステップをさらに含んでもよい。

【0076】図13は、ショッピングシステム15におけるデジタル証明書の検証手順を示すフローチャートである。電子商取引部70はユーザシステム30から取引要求とともにユーザの証明書を受信する(S40)。CA公開鍵管理部74は受信した証明書の完全性を検証するために、証明書を発行したCAである認証装置26へ公開鍵を要求する(S42)。証明書検証部72はCA公開鍵により証明書のデジタル署名を復号し、署名を検証する(S42)。CAの署名の正当性が検証された場合(S42のY)、電子商取引部70はユーザシステム30に取引開始確認を送信し、ユーザシステム30との取引を実行し(S44)、CAの署名の正当性が否定された場合(S42のN)、ユーザシステム30との取引を拒否する(S46)。

【0077】ユーザシステム30とショップシステム15は、ユーザとオンラインショップとの間の電子商取引をデジタル証明書を用いて安全に行うための専用ソフトウェアとして実現することができる。この場合、とくにユーザ端末28側にインストールされるユーザシステム30のプログラムは、ハードウェア固有情報の検証ルーチンが不正に改変されないようにプログラムコードの難読化などの改変防止対策が取られる。

【0078】以上述べたように、本認証システムは、ユーザが使用しているハードウェア情報を付加したデジタル証明書を使用して認証を行うシステムである。主に電子商取引での利用を目的としている。なぜなら、セキュリティに関心がないユーザがコンピュータを使ってインターネットに接続してオンラインショッピングを楽しんでおり、ユーザ自身が扱うID・パスワードが簡単に漏れてしまうことが多く、不正行為も容易に出来てしまうからである。それを抑制するためにコンピュータ側で認証情報を管理する必要がある。ID・パスワードだけの認証情報では不正行為を抑止することは困難であるため、不変なユーザ情報としてPSN、MACアドレス等のハードウェア固有情報を用いた。本認証システムを利用することで、サービスを提供する側もユーザ自身もより安全で容易に電子商取引を行うことができる。

【0079】また本認証システムは、標準的なOSの上にアプリケーションレベルで開発できるため、実装に手間がかからず、またICカードによる認証や指紋認証とは違い、認証のための特別なハードウェアを必要としない。また本認証システムではユーザが使用するハードウェアが盗まれない限り、「なりすまし」ができない。ユーザは認証データを盗まれて気がつかないが、自分の使っているハードウェアの盗難は早期に発見できるため、不正利用に対して直ちに対処できる。

【0080】また本認証システムでは、ユーザの個人情報を管理してユーザにネットワークサービスを提供するISPなどの組織が認証局は兼ねるため、ユーザの属する組織ごとに分散された認証局を比較的簡単な構成で立ち上げることができる。

【0081】以上、本発明を実施の形態をもとに説明した。実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能でなく、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。以下そのような変形例を説明する。

【0082】本認証システムはPCベースのシステムに限られない。PCの普及率は飽和状態にあり、その代わり携帯端末の普及が目覚ましい。本システムはPDA(Personal Digital Assistance)と総称される携帯端末機や、携帯電話に应用することができる。最近、一部の携帯電話でJava(登録商標)アプリケーションが動作するようになってきており、今後全ての携帯電話の標準

的な機能となると思われる。また、各携帯電話は必ず固有IDを持っており、この固有情報とJava技術を利用することにより、デジタル証明書を利用した認証システムを構築することができる。

【0083】また上記では一般的な例としてWeb上での電子商取引においてデジタル証明書を利用する場合を説明したが、もちろんWebに限定する趣旨ではない。またデジタル証明書は電子商取引に限らず、公的書類の申請や発行、税金等の手続きなど商取引以外の場面でも利用される。そのような場合においても本発明の認証システムを適用することにより、なりすましなどの不正行為を防止することができる。

【0084】また本認証システムはユーザの属する組織単位で分散した認証局を用いるため、ユーザ全体を統一して管理する必要はなく、認証局ごとに異なる認証方式を採用することもできる。また組織単位でユーザを認証可能であればよいので、組織内でユーザをユニークに識別できる固有の識別情報をデジタル証明書に用いることで十分である。したがってPSNのように完全にユニークな識別情報を使わなくても、MACアドレスやハードウェアのシリアルナンバー、ハードウェアのコンフィグレーションなど、他の識別情報を組合せたり、それらの識別情報の一部を用いることで対処することも可能である。また識別情報として、BIOSのバージョンやROMに書き込まれた製品のロットナンバーなどを用いてもよい。

#### 【0085】

【発明の効果】本発明によれば、ユーザ認証における不正行為を防止することができる。

#### 【図面の簡単な説明】

【図1】 実施の形態に係るデジタル証明書のデータの構造を説明する図である。

【図2】 プロセッサシリアルナンバーの表示画面を説明する図である。

【図3】 実施の形態に係るデジタル証明書の申請と発行の手順を説明する図である。

【図4】 実施の形態に係る認証システムにおける商取引の手順を説明する図である。

【図5】 実施の形態に係る証明書の管理と認証の手順を説明する図である。

【図6】 実施の形態に係る認証システムの構成図である。

【図7】 図6の認証装置の構成図である。

【図8】 図6のユーザシステムの構成図である。

【図9】 図6のショップシステムの構成図である。

【図10】 認証装置におけるデジタル証明書の生成と発行の手順を示すフローチャートである。

【図11】 ユーザシステムにおける証明書発行要求の手順を示すフローチャートである。

【図12】 ユーザシステムにおけるハードウェア固有

情報の検証手順を示すフローチャートである。

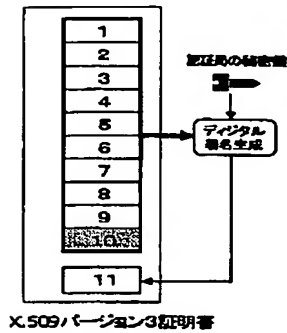
【図13】 ショップシステムにおけるデジタル証明書の検証手順を示すフローチャートである。

【符号の説明】

10 オンラインショッピングサイト、 12 Webサーバ、 14 データベースサーバ、 15 ショップシステム、 16 インターネット、 18 インターネットサービスプロバイダ、 26 認証装置、 28 ユーザ端末、 30 ユーザシステム、 32 証明

書生成部、 34 鍵生成部、 36 ダイジェスト生成部、 38 デジタル署名部、 40 証明書発行部、 42 証明書データベース、 44 公開鍵配布部、 50 証明書管理部、 52 鍵ペア生成部、 54 証明書要求生成部、 56 証明書保持部、 58 証明書受信部、 60 ハードウェア固有情報取得部、 62 ハードウェア固有情報検証部、 64 電子商取引部、 70 電子商取引部、 72 証明書検証部、 74 CA公開鍵管理部。

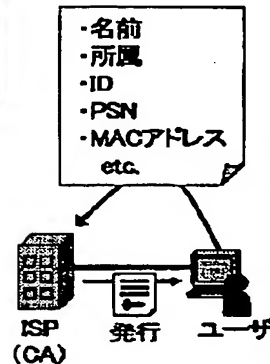
【図1】



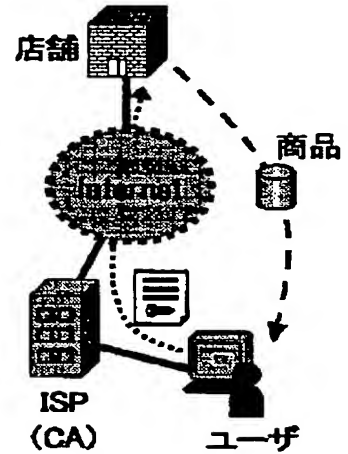
【図2】



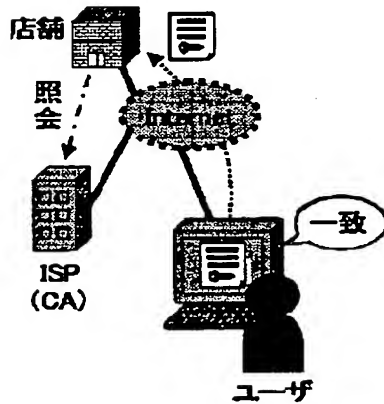
【図3】



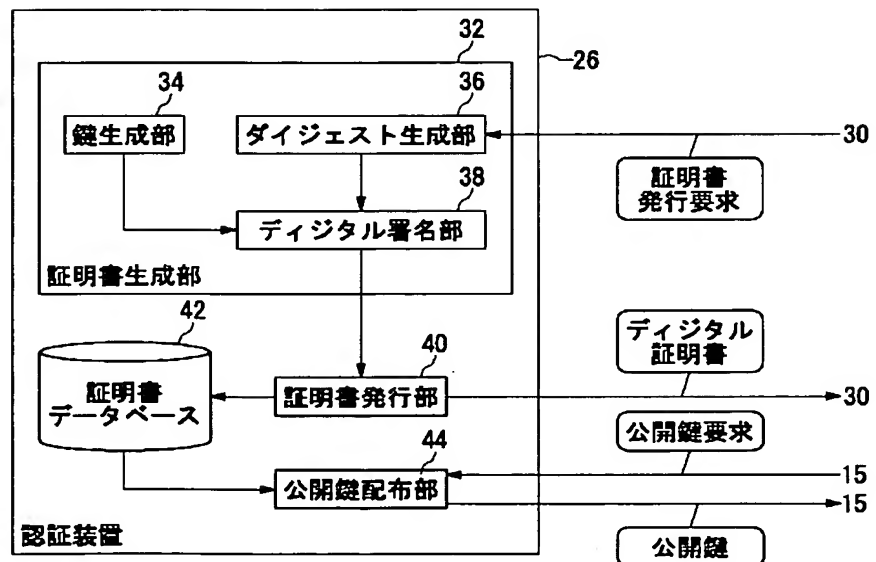
【図4】



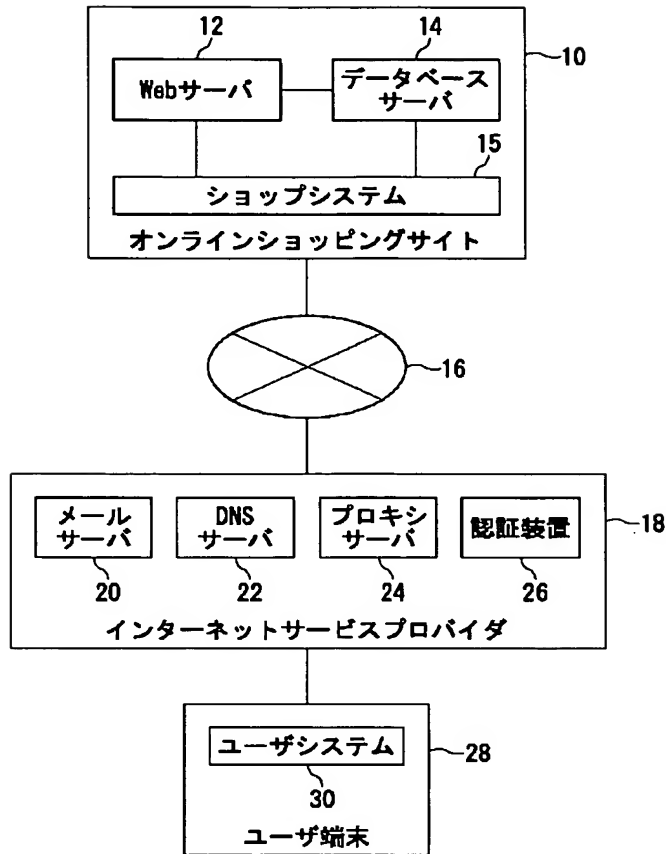
【図5】



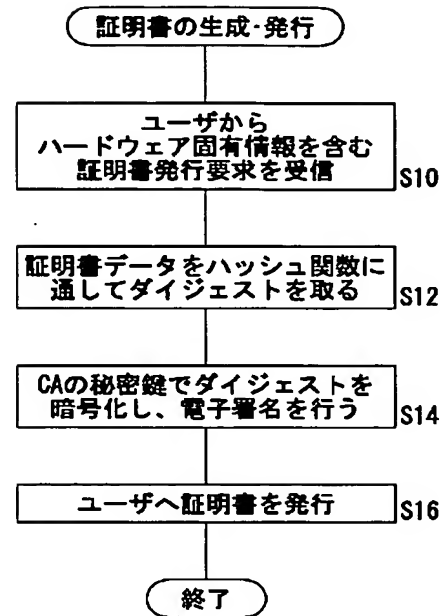
【図7】



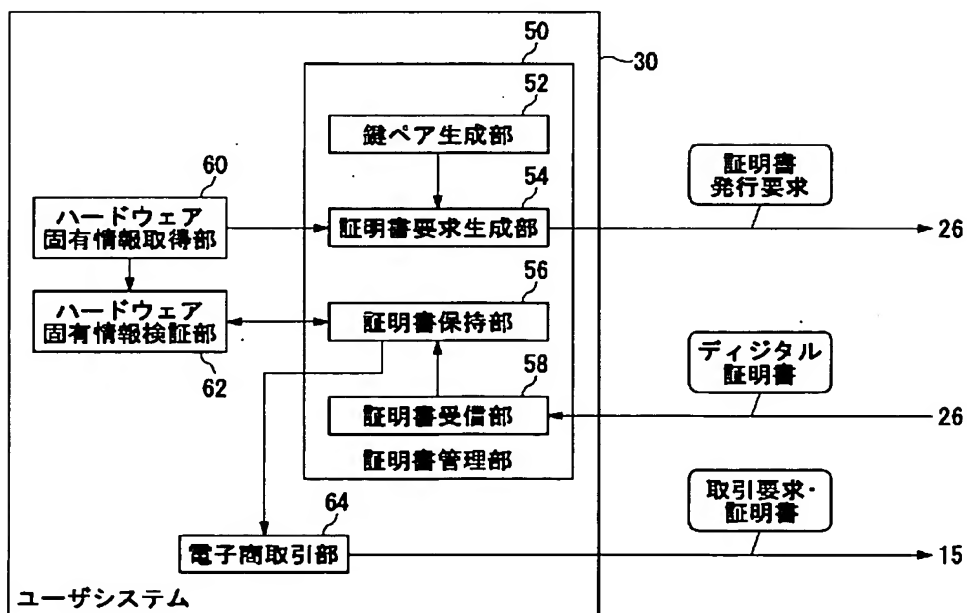
【図6】



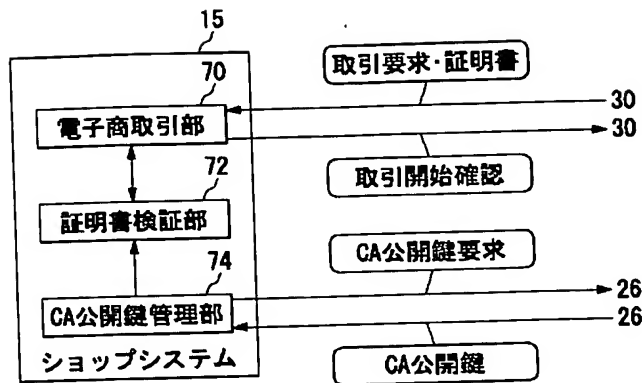
【図10】



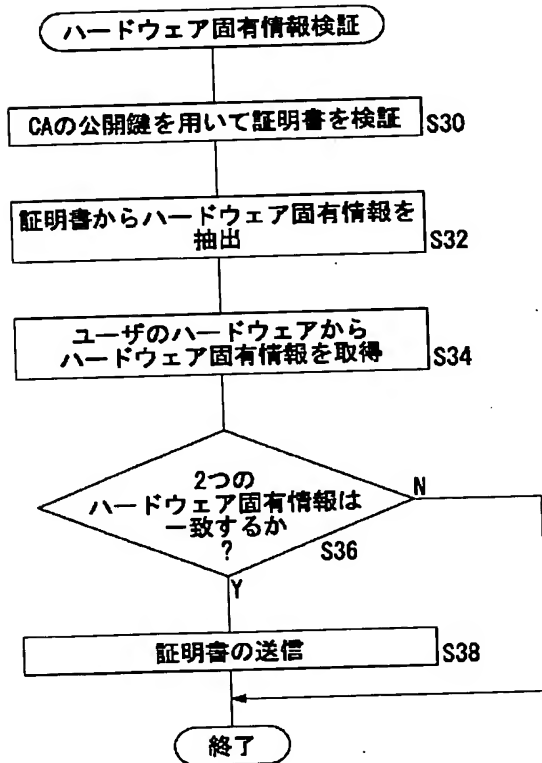
【図8】



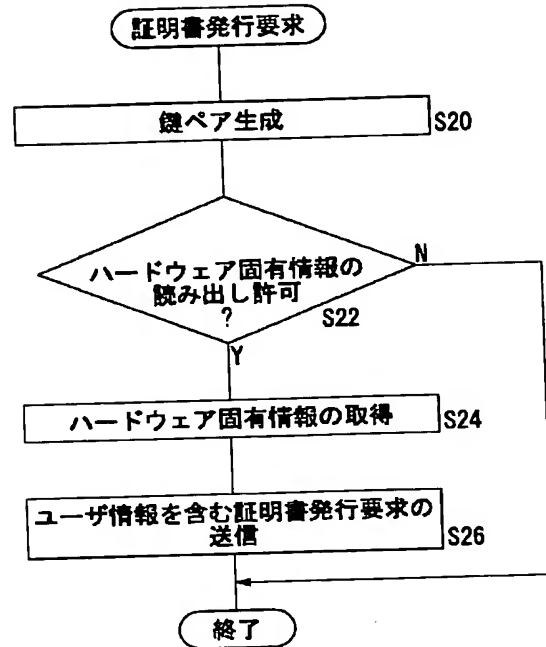
【図9】



【図12】



【図11】



【図13】

